Department Of Defense Information Technology Security Certification and Accreditation Process (DITSCAP)

Prototype
SSAA Preparation Tool
Supplement to DoD Manual 5200.40-M

May 18, 1999
Version 1

Prepared for:
Defense Information System Agency

Prepared by:
Corbett Technologies, Inc.
2121 Eisenhower Avenue, Suite 200
Alexandria, VA 22314-4685

Introduction

This System Security Authorization Agreement (SSAA) Preparation Tool has been developed to assist in the preparation of SSAAs in accordance with the requirements described in the DITSCAP (Department of Defense Information Technology Security Certification and Accreditation Process), DoD Inst 5200.40, and its companion DITSCAP Application Document, DoD Manual 5200.40-M. It follows the prescribed outline of a DITSCAP compliant SSAA, paragraph by paragraph. Each paragraph is preceded by applicable directions taken from the Application Document, followed by references and links to the Application Document where additional guidance may be found if required.

A generic example of the type of information and the level of detail that should be incorporated in the paragraph follows. Most of the examples in the body of this version of the tool are based upon a hypothetical model of a system that is described in Section 1 and 3. This hypothetical model is designed to be representative of a large class of DoD systems. In some cases within the body of the tool, and in the Examples Addendum to the tool, we have included sanitized text taken from worked examples of SSAAs prepared for actual systems. These examples are intended to provide guidance and suggestions to the user of the tool, but, in all cases the language must be modified and adapted to the details of the system for which the SSAA is being prepared. An automated link between the paragraph of the tool and the appropriate additional examples in the addendum is provided. This link is actuated by clicking on the highlighted phrase: "*For more examples, see Examples_Addendum.*"

This first version of the tool is a prototype and does not contain a complete set of examples and has not been completely edited for consistency. It is intended to demonstrate the utility of such a tool to support the preparation of DoD SSAAs that comply with the requirements of the DITSCAP and to serve as a basis for the development of a tool that can be distributed to the DoD community.

To use the tool:

1. Each section of the SSAA Preparation Tool contains the basic instructions for completing that section. **Review the instruction**. If additional instructions are needed, select the link to the Application Document for more detailed information.
2. **Review the worked example**. This should enhance your understanding of the information that needs to be included in this section.
3. **Delete the words, "Type your Text here**," and then **enter your information**.
4. **Complete all sections of the DITSCAP.**
5. **Delete the preparation instructions, the examples and the links** to the Application Document and to the Examples_Addendum.
6. **Run spell and grammar check** as appropriate.
7. **Regenerate the Table of Contents.**

Table of Contents

1.0 MISSION DESCRIPTION AND SYSTEM INDENTIFICATION

1.1 System Name and Identification

Identify the target system that is being developed or entering the C&A process. Provide the name, organization, and location of the element developing the mission need and the organizations containing the ultimate user. Identify the general user who helps to define operational scenarios that may be encountered.

For additional information, see DITSCAP Application Document, Section C3.3.1

Example:

The COMMAND SYSTEM/NETWORK is the subject of this System Security Authorization Agreement (SSAA). The COMMAND ELEMENT of the COMMAND, located at FORT ABC was responsible for the development of the mission need for the COMMAND SYSTEM/NETWORK. Users of the system are personnel of UNIT A, UNIT B, AND UNIT C of COMMAND.

For more examples, see Examples_Addendum.

Type your text here.

1.2 SYSTEM DESCRIPTION

Provide a complete high-level description of the system architecture, including diagrams or drawings to amplify the description. Describe all components of the system. The description should include all critical elements required for the mission need.

For additional information, see DITSCAP Application Document, Section C3.3.1.2

Example:

COMMAND SYSTEM/NETWORK is a general support system providing office automation tools to COMMAND administrative, investigative, analytical and technical support personnel in carrying out their mission related functions. Administrative support is facilitated through the use of COTS applications such as MS Word, Excel, PowerPoint, Exchange E-mail, and the COMMAND SYSTEM/NETWORK Web Browser (Netscape). COMMAND SYSTEM/NETWORK provides access to databases and other information resources of the COMMAND SYSTEM/NETWORK network servers and the ABC Database, maintained under the Oracle database management system (DBMS) on the COMMAND SYSTEM/NETWORK UNIX Server.

The COMMAND SYSTEM/NETWORK system embodies an open architecture designed to accommodate the rapid introduction into the system of advanced information processing resources. The architecture organizes the COMMAND SYSTEM/NETWORK local area network (LAN) resources into two interconnected high speed Ethernet fiber digital device interface (FDDI) rings located in separate buildings. The LANs are connected by a fiber optic link enclosed within a protected distribution system (PDS). Each LAN ring includes a variety of communications equipment (routers, switches, concentrators, etc.) and up to N workstations. COMMAND SYSTEM/NETWORK network servers and the domain controller consist of three Hewlett Packard Pentium II 400 MHz computers using the Windows NT 4.0 Operating System. The Oracle database server is hosted on a SUN Ultra 6000 Server using SUNSolaris 2.6 operating system. The two interconnected LAN rings comprise the single domain of the COMMAND SYSTEM/NETWORK operating environment.

Users access the system through individual Pentium desktop workstations that are installed throughout buildings A and B of the COMMAND HQ complex. Each workstation is connected to one of the LAN rings. Workstations use the Windows98 operating system supported by shared HP LaserJet 4 printers and desktop scanners.

The COMMAND SYSTEM/NETWORK LAN operating environment interfaces with each of the COMMAND SUB-UNIT LANs. These are interconnected through dedicated encrypted commercial carrier T-1 links that make up the COMMAND Wide Area Network (WAN). The COMMAND SYSTEM/NETWORK also interfaces with the DoD Secret Internet Protocol Network (SIPRNet). See 3.4 below for a description of network interconnections.

Figure 1-1 provides a conceptual overview of the COMMAND SYSTEM/NETWORK.

For more examples, see Examples_Addendum.

Type your text here.

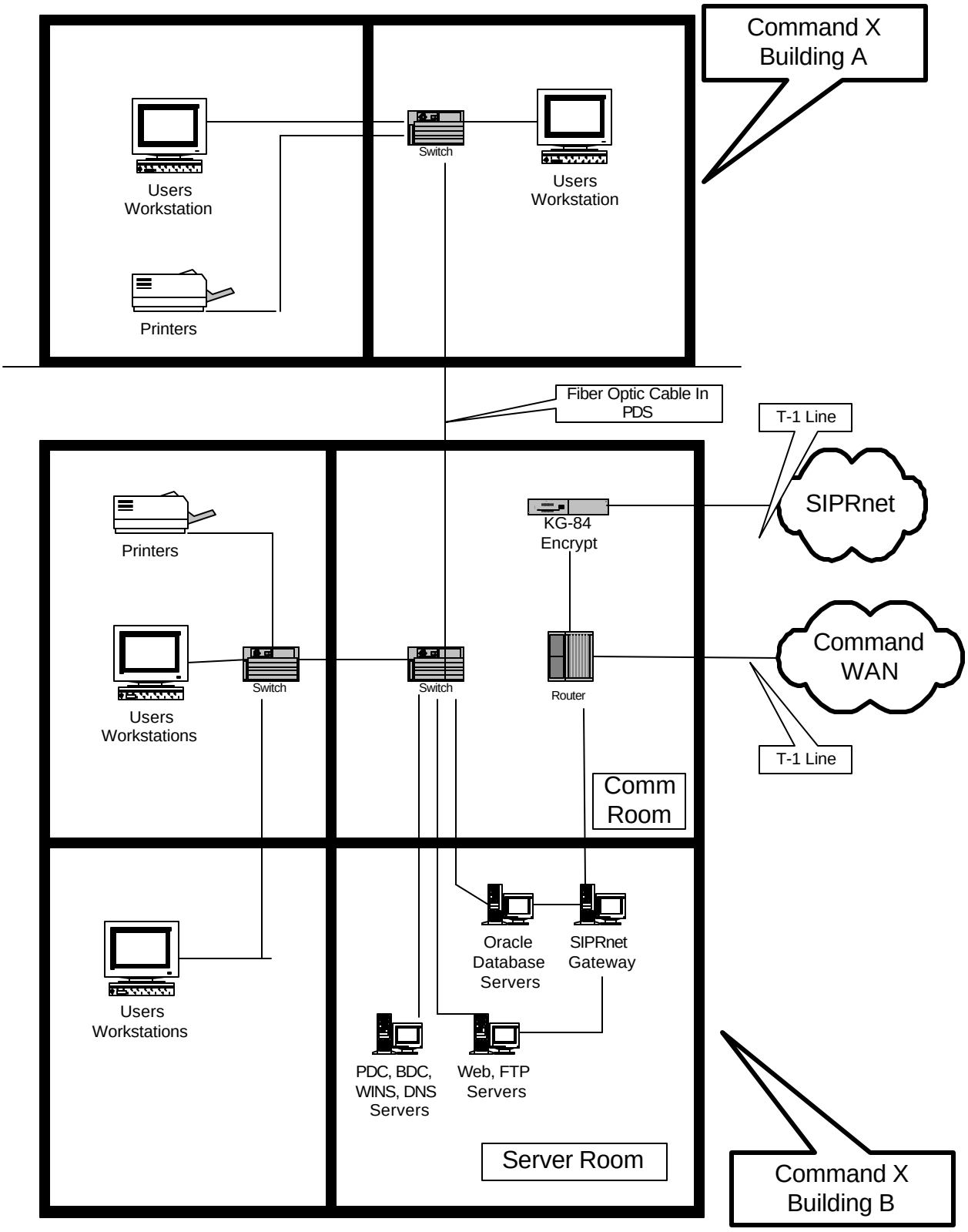

Figure 1-1: Conceptual Overview of COMMAND SYSTEM/NETWORK

1.3 FUNCTIONAL DESCRIPTION

1.3.1 System Capabilities

Clearly define the functions or capabilities expected in the fully accredited system and the mission for which it will be used. Include functional diagrams of the system. Provide the intended flows of data into the system, data manipulation, and product output.

For additional information, see the DITSCAP Application Document, Section C3.3.1.2.2.

Example:

All *COMMAND SYSTEM/NETWORK* users are granted access to a standard configuration of automated tools on the system/network The standard tools are:

- *WordPerfect (for general document preparation)*
- *Microsoft Word (not approved for formal COMMAND usage, but available for general document preparation)*
- *Microsoft Excel (spreadsheet functionality)*
- *Microsoft PowerPoint (graphics capability)*
- *FormPrep (COMMAND forms and administrative functions)*
- *COMMAND SYSTEM/NETWORK Web Browser (Netscape) (a full text search capability for searching the files stored in electronic form)*
- *Windows accessories (provides additional utilities such as Calculator, Notepad, MS Paint, Spell Checker, Thesaurus, etc.)*
- *Microsoft Outlook (electronic mail capability)*

COMMAND SYSTEM/NETWORK is designed to provide automated support to all facets of *COMMAND HQ* administrative and mission support functions. It provides *COMMAND* personnel the capability to prepare, disseminate and electronically store and retrieve all types of documents and personnel and fiscal records required to be generated, filed and maintained in support of the operations of *COMMAND HQ.*

COMMAND SYSTEM/NETWORK also supports the capability to create and maintain relational databases under the *Oracle* DBMS installed on the database server in the *COMMAND SYSTEM/NETWORK* computer room. At present these consist of the following:

Database Name	Database Contents	Function(s) Supported

COMMAND SYSTEM/NETWORK provides E-mail services to all *COMMAND* HQ personnel, either through the *COMMAND* HQ LAN or across the *COMMAND* T1 WAN. *COMMAND SYSTEM/NETWORK* users can also exchange E-mail with other *COMMAND* personnel that are still using the Wang office automation system. In addition, the Classified *COMMAND SYSTEM/NETWORK* System has been designed to provide the capability for the *COMMAND SYSTEM/NETWORK* and the unclassified *COMMAND SYSTEM/NETWORK* users to exchange E-mail at the unclassified and unclassified but sensitive levels through a Classified *COMMAND SYSTEM/NETWORK* trusted gateway planned for installation in the future.

For more examples, see Examples_Addendum.

Type your text here.

1.3.2 SYSTEM CRITICALITY

Define the system criticality and the acceptable risk for the system in meeting the mission responsibilities. System criticality should consider the impact if the system were not operational.

For additional information, see the DITSCAP Application Document, Section C3.3.1.2.2.1.

Example:

COMMAND SYSTEM/NETWORK supports the creation of and provides on-line storage of a large variety of information supporting all facets of the COMMAND mission. Critical COMMAND information is, at a minimum, considered sensitive, and a large body of the information processed by the system is subject to the Privacy Act (PA). The system may also contain proprietary information. In addition, a considerable portion of the information created on and processed by the system is NSI that is classified at either the Confidential or Secret levels. Since the mode of operation of the system is system high Secret, all COMMAND SYSTEM/NETWORK data must be protected at the Secret security level unless and until it has been manually reviewed and downgraded or declassified. The eventual interface between COMMAND SYSTEM/NETWORK and the SBU COMMAND SYSTEM/NETWORK is addressed in greater detail in Section 3.

For more examples, see Examples_Addendum.

Type your text here.

1.3.3 CLASSIFICATION AND SENSITIVITY OF DATA PROCESSED

Define the type and sensitivity of the data processed by the system. Examine the mission need to determine the national security classification of information to be processes (unclassified, confidential, secret, and top secret) along with any special compartment. Special handling requirements must also be identified. Identify the type of information processed (Privacy Act, financial, critical operational, proprietary, and administrative).

For additional information, see DITSCAP Application Document, Section C3.3.1.2.2.2.

Example:

InfoSystem provides on-line storage of a large variety of ABC information supporting all facets of the ABC mission. Critical ABC information is, at a minimum, considered sensitive and a large body of the information processed by the system is subject to the Privacy Act (PA). The system may also contain proprietary information. Material contained in ABC investigative case files is particularly sensitive in that much of it will be required to support legal prosecutions of individuals by the US Attorney's Offices and must be protected from loss, corruption, or premature disclosure. Of extreme sensitivity, is the information on ABC informants that the system will contain. Unauthorized disclosure of this information is life threatening. Thus, all InfoSystem data must be protected at the unclassified but sensitive security level. It should be noted that while InfoSystem processes unclassified but sensitive information, the Classified InfoSystem system, which processes SECRET information will use InfoSystem communications circuits. The eventual interface between InfoSystem and Classified InfoSystem is addressed in greater detail in Section 3.

For more examples, see Examples_Addendum.

1.3.4 System User Description and Clearance Levels

Define the system user's security clearances, their access to specific categories of information processed, and the actual information that the system is required to process. If the system's authorized users include contractor personnel, indicate how proprietary information will be protected.

For additional information, see DITSCAP Application Document, Section C3.3.1.2.2.3.

Example:

All persons who have access to or are users of the COMMAND SYSTEM/NETWORK have a DoD Secret or higher security clearance. The users are cleared employees of the COMMAND or cleared support contract personnel. The workstations are administered and operated by the

COMMAND classified LAN personnel and their support contractors. Access to all databases or other information repositories that may contain proprietary information is controlled by DAC mechanisms that limit access to COMMAND employees and preclude access by contract personnel.

For more examples, see Examples_Addendum.

Type your text here.

1.3.5 Life Cycle of the System

Define the system life cycle and where the system is in relationship to its life cycle.

For additional information, see DITSCAP Application Document, Section C3.3.1.2.2.4.

Example:

COMMAND SYSTEM/NETWORK has achieved an Initial Operating Capability (IOC) and is currently in operation at COMMAND HQ under an Interim Authority to Operate (IATO). The system is under continued development, with Final Operating Capability (FOC), following system Test and Evaluation (T&E) and Government acceptance, now scheduled for the end of calendar year 2000. Upon acceptance by the Government the system will be placed under configuration control of the COMMAND CONFIGURATION CONTROL BOARD. Maintenance of the system will be provided by a contractor and will require that on-site maintenance be supported through use of automated test and diagnostic equipment that will isolate problems to the X level. The maintenance concept for on-site repair will be isolation and replacement of faulty components. Faulty components will be transferred to a contractor facility for repair or replacement. On-site maintenance personnel will be required to be cleared, at a minimum to the DoD Secret level. Before being released from Government custody and control, all defective system components containing non-volatile memory will be sanitized using DoD and Command approved sanitization methods for Secret level equipment.

For more examples, see Examples_Addendum.

Type your text here.

1.4 SYSTEM CONOPS SUMMARY

Describe the system concept of operations (CONOPS), including functions performed jointly with other systems. Identify the other systems. Many systems will have a document that describes the system CONOPS. If so, include a short summary in the SSAA and add the CONOPS document as an appendix or list as a reference.

For additional information, see DITSCAP Application Document, Section C3.3.1.2.3.

Example:

The concept of operations of the COMMAND SYSTEM/NETWORK is to provide a processing environment where COMMAND personnel (government and authorized contractors) can accomplish the automated processing and office automation support associated with operations, research and support prescribed by the COMMAND mission.

Information is made available to COMMAND users by processing applications against databases and by an Intranet which uses Web technology. Authorized COMMAND users have been given accounts on the various COMMAND AIS resources. Each authorized user must enter an appropriate I&A before being authorized access to the COMMAND AIS resources. The requirement for an I&A is the first line of defense for ensuring that only authorized personnel have access to COMMAND data and AIS resources.

COMMAND SYSTEM/NETWORK users are also provided the capability of exchanging E-mail with other COMMAND users of the COMMAND SYSTEM/NETWORK and with other COMMAND personnel across the COMMAND WAN. Users are also provided access to information system resources through the DoD SIPRNet. For more detailed information concerning the COMMAND SYSTEM/NETWORK CONOPS see Reference n/Appendix X.

For more examples, see Examples_Addendum.

Type your text here.

2.0 ENVIRONMENT DESCRIPTION

This section is blank; it is a title.

For additional information, see DITSCAP Application Document, Section 3.3.3.

2.1 OPERATING ENVIRONMENT

Provide an overview of the operating environment.

For additional information, see DITSCAP Application Document, Section 3.3.3.2.1.

Example:

The COMMAND SYSTEM/NETWORK operating environment is a complex integration of COMMAND operational and support personnel, who provide management direction and oversight to support and operations of the COMMAND at COMMAND HQ. This integrated effort harmonizes the security protection provided at the COMMAND HQ Buildings with the system development, integration, and maintenance of the COMMAND SYSTEM/NETWORK in response to a recognized threats.

For more examples, see Examples_Addendum.

Type your test here.

2.1.1 Facility Description

Describe the physical environment in which the system will operate including floor plans, equipment placement, electrical and plumbing outlets, telephone outlets, air conditioning vents, sprinkler systems, fences, and extension of walls from true floor to true ceiling.

For additional information, see DITSCAP Application Document, Section C3.3.3.2.1.1.

Example:

The *COMMAND SYSTEM/NETWORK* is located in Rooms *X, X, X*, and *X* in Building *B*, and Rooms *X* and *X* in building *A* at *Fort ABC* which is a *Command* access controlled facility enclosed with fences and with guard protection at all vehicular entrances. *(Describe type and construction of buildings)*

For more examples, see Examples_Addendum.

Type your text here.

2.1.2 Physical Security

Identify the procedures needed to counter potential threats that may come from inside or outside the organization.

For additional information, see DITSCAP Application Document, Section C3.3.3.2.1.2.

Example:

All entrances to the buildings in which COMMAND SYSTEM/NETWORK resources are located are protected by the COMMAND guard force twenty-four hours per day, seven days per week. All persons with unescorted access to the building must be cleared, at a minimum, to the Secret level and badged. Entrance to the server room and the communications room in Building B is controlled by cipher locks. Persons with unescorted access to these rooms are limited to COMMAND personnel whose duties require entrance to these rooms and to contractor maintenance personnel who are cleared to the Secret level. In addition, all persons with unescorted access to the communications room must also possess a COMSEC clearance. All such persons must be on an access control list maintained in each of these rooms. All visitors not on the access control list must be continually escorted by authorized COMMAND personnel and signed in and out by their escorts.

Physical security of the rooms and buildings in which the equipment of COMMAND SYSTEM/NETWORK is located conform to COMMAND standards listed in reference n. A COMMAND staff member is appointed as the Physical Security Monitor for the facility and ensures COMMAND requirements are understood and enforced. The security guards in buildings A and B hold the combinations to Rooms X and X in Building A and Rooms X and X in Building B. COMMAND SYSTEM/NETWORK personnel possess the door keys and cipher combinations to Room X, the server room, and Room X, the Communications Room, in Building B.

Figure 2-1 and 2-2 show the above described rooms in buildings A and B, respectively, with one door with a built-in, DoD-approved combination lock. Each room has true floor-to-ceiling walls, and Rooms X and X in building A and Rooms X and X in building B have windows. The windows are covered with curtains and no monitor faces the windows. Rooms X and X in building B meet all COMMAND requirements for open storage of Secret information and are designated in writing for such storage.

Insert Figures

Alarms and sensors, as indicated in Figure 2-2, enhance the security of the COMMAND SYSTEM/NETWORK servers and communications equipment in Rooms X and X. The sensors are monitored by the COMMAND protective service force located in Address. The guard force monitors the sensor alarms 24 hours a day, 7 days a week. Should an alarm be activated a

guards immediately investigate and call the site manager. The site manager will determine if an COMMAND SYSTEM/NETWORK staff member will need to be called in to perform a physical inspection of Rooms X and X.

Buildings A and B are equipped with sprinkler systems and contain adequate water drainage systems, but lack water sensors. No fire or water-related incidents have ever occurred in either building.

For more examples, see Examples_Addendum.

Type your text here.

2.1.3 Administrative Security

Identify the routine office security practices that ensure unauthorized access to protected resources is prohibited.

For additional information, see DITSCAP Application Document, Section C3.3.3.2.1.2.

Example:

All system output must be appropriately labeled. In rooms that are not approved for the open storage of Secret level NSI, all classified system output must be stored in GSA approved safes that are provided for such purposes. Checklists for the opening and closing of the safes are provided and maintained and the rooms are periodically checked by the guard force during non-duty hours.

The steel conduit that constitutes the PDS for the fiber optic link between Building A and Building B is visually checked daily for any evidence of tampering.

Type your text here.

2.1.4 Maintenance Procedures

Identify routine maintenance procedures and the number of personnel required to maintain the system. Certain categories of information mandate special maintenance procedures to ensure physical security protection against unauthorized access to the information or system resources.

For additional information, see DITSCAP Application Document, Section C3.3.3.2.1.3.

Example:

Routine maintenance of all COMMAND SYSTEM/NETWORK hardware and software is performed by two appropriately cleared COMMAND technical personnel and COMMAND SYSTEM/NETWORK system administration personnel. In addition, there is a contract in place with ABC, Inc., for on-call maintenance of COMMAND SYSTEM/NETWORK hardware with a minimum response time of 8 hours. ABC. Inc., maintains a staff of appropriately cleared personnel possessing the technical competence to perform maintenance on all types of COMMAND SYSTEM/NETWORK equipment.

Type your text here.

2.1.5 Training Plans

Identify the training provided to the individuals associated with the system's operation and determine if the training is appropriate to their level and area of responsibility.

For additional information, see DITSCAP Application Document, Section C3.3.3.2.1.4.

Example:

All DoD elements should have existing training plans that cover INFOSEC training. If such plans are concise, they can be inserted here verbatim. If deemed too extensive for incorporation here they should be summarized here and incorporated by reference or they can be attached as an additional appendix and referred to in this paragraph.

Type your text here.

2.2 SOFTWARE DEVELOPMENT AND MAINTENANCE ENVIRONMENT

Describe the system development approach and the environment within which the system will be developed. Describe the information access and configuration control issues for the system. Identify is the system development and maintenance environment is opened or closed.

For additional information, see DITSCAP Application Document, Section C3.3.3.2.2.

Example:

The software that is employed by the COMMAND consists of commercial off-the-shelf (COTS) products and an application, Y APPLICATION, developed by the COMMAND SYSTEM/NETWORK integration contractor. During the development of COMMAND SYSTEM/NETWORK, the integration contractor is responsible for the acquisition and integration of COTS products specified and approved for incorporation in the system and for the maintenance of Y APPLICATION under the supervision of the Program Manager. Upon attainment of IOC and acceptance of the system by the Government, all software will be maintained and upgraded by COMMAND SYSTEM/NETWORK operational staff under the supervision and control of COMMAND CONFIGURATION CONTROL BOARD.

For more examples, see Examples_Addendum.

Type your text here.

2.3 THREAT DESCRIPTION

Describe the potential threats to the Command System/Network and data at the Command HQ and Command Sites and address the threat environment and single points of failure in the system. These are threats to the integrity, confidentiality, and availability of the system. Clearly state the nature of the threat that is expected and wherever possible, the expected frequency of occurrence. Unintentional human error, system design weaknesses and intentional actions on the part of authorized as well as unauthorized users can cause these events. Generic threat information is available, but it must be adapted to clearly state the threats expected to be encountered by the system. Evaluate the degree of threat to the system. Conduct a risk analysis, then identify appropriate cost-effective countermeasures to mitigate the risk.

For additional information, see DITSCAP Application Document, Section C3.3.3.2.3.

2.3.1 Threat Description

This description amplifies the findings of the National Security Telecommunications and Information Systems Security Committee (NSTISSC) as reported in its Annual Assessments of the Status of National Security Telecommunications and Information Systems Security within the United States Government.

> *Note: The foregoing paragraph should state all of the sources from which the system specific threat statement has been derived. The NSTISSC 'Annual Assessment' has not been issued for several years, but still constitutes one of the most comprehensive and authoritative statements of the threat to national security information systems and networks. More current threat statements should be available from the National Counterintelligence Center (NACIC), Threat Assessment Office - Tel. No. (703) 874-4119*

Unclassified FAX No. (703) 874-5844, Secure FAX No. (703) 874-5929. The NACIC operates under the auspices of the National Security Council and draws its staffing from the FBI, CIA, DIA, NSA, OSD, the services, DOS and DOE. Additional support in this area is available from DISA, POC_____. (After talking with the NACIC, it seems that they only 'do' tailored assessments under tasking through the appropriate chain of command, suggesting that DoD elements should go through the service intelligence branches/agencies, in other words, no real help in this area. They were not aware of any re-issuance of the NSTISSC threat or any similar national level threat document.

The threat of outside intrusion into the *Command System/Network* is considered to be *(high/medium/low).* At present, this threat is substantially negated by the restrictions on outside communications links and encryption of all communications between *Command System/Network* sites. The principal threat to *Command* data communications and information systems is adjudged to be the insider threat. Because of *(insert rationale),* the threat of cooption of authorized *Command System/Network* users by hostile agents is deemed to be *(high/medium).* This assessment is supported by the fact that recent compromises of intelligence and national security information have occurred through the medium of insiders with authorized system accesses who have disclosed classified information primarily for the purposes of financial gain. The insider threat arises from multiple sources and is manifested in various ways. There is the threat of the cooption of users with authorized access to the system. Such users may be contractor support personnel or *Command* personnel with physical access to the system components. These users may be motivated by financial gain or personal reasons. Disgruntled personnel, especially those who are to be terminated for cause, pose another threat. There is also the threat posed by users of the system who negligently or inadvertently fail to follow security rules or procedures. These security rules and procedures include:

- Requirements for the handling and labeling of system output or media,
- ? The location of *Command System/Network* resources in controlled access spaces.
- The rules against the introduction of unauthorized software or data imported from unauthorized sources.

Finally, there is the threat arising from the failure of authorized users to employ proper procedures for the entry or manipulation of system data. This may arise out of negligence or from the failure of users to be properly trained in the use and operation of the system.

These insider threats can be manifested in the following ways:

- Unauthorized reading, copying or disclosure of sensitive or classified information,
- Execution of denial of services attacks,
- Introduction into the system of viruses, worms or other malicious software,
- Destruction or corruption of data,
- Sabotage,
- Exposure of sensitive *or classified* data to compromise through the improper labeling or handling of printed output, or

- Improper labeling or handling of magnetic media resulting in the compromise of sensitive *or classified information*.
- Introduction into the system of information of a higher sensitivity level than that authorized for the system.
- Making unauthorized connections to insecure or clandestine communications links or other systems of a lower level of sensitivity or classification.

The coopted insider would most likely copy to floppy diskettes and remove from the system any and all types of sensitive or classified information to which he or she had access. A user might also probe the system in an attempt to discover ways to circumvent access permissions and copy and remove from the system sensitive *or classified* information. This might be attempted by a user who was an extremely sophisticated hacker (or under the direction and control of such a person) by introducing "sniffer" software into the system to learn the user ID and password of a system administrator or other privileged users. If successful, a hacker could then bypass access controls and gain access to the most sensitive information on the system. In most instances of these attacks, there could well be attempts to modify audit data and prevent analysis and detection of the source and nature of the attack. The most serious of all possible attacks against the system could be committed by systems or security administration personnel, who have the ability to alter or bypass most, if not all, of the system's technical protection mechanisms.

In addition, either a coopted insider or disgruntled personnel might attempt denial of service attacks through the manipulation of system software or the malicious introduction into the system of viruses, worms or other destructive software. Authorized users might also maliciously modify data stored on the system to undermine confidence in the integrity of the system and the accuracy of its stored information. Although unlikely, there is always at least a minimal threat of sabotage. There could be attempts by insiders with physical access to *Command System/Network* resources, whether or not they are authorized users, to tap the network communications links in order to record and extract data from the system.

The NSTISSC Assessment documents the high level threat to U.S. Government information and telecommunications systems from hackers, particularly on the Internet. In the past, there have been numerous documented successful hacker attacks on the central switching nodes of the public switched network. However, the use of *(STU-III equipment with the Security Access Control System (SACS) option enabled for dial-in connections, together with the exclusive use of FTS 2000 links which incorporate NSA approved Type 1 encryption encrypting all Command System/Network traffic that is transmitted over the Command WAN) or (other similar statement of effective countermeasures),* negates any such threat to inter-site communications.

Despite the end of the Cold War, the general threat to United States national security from foreign government intelligence activities remains high. *(Because of the extreme sensitivity of the information processed by the Command System/Network/ its potential value to foreign governments/ its criticality to the mission of Command it is likely that Command System/Network may be the target of penetration or denial of service attacks by hostile foreign intelligence services) or* (*Nevertheless, because of the low level of sensitivity of the information processed by Command System/Network and the marginal value of the information to foreign governments/the low level of criticality to the mission of Command it is unlikely that Command System/Network*

would be the target of penetration or denial of service attacks by any hostile foreign intelligence service) or (other similar statement tailored to the particular circumstances of the system/network that is the subject of the SSAA).

A recent report of a threat assessment of *Command* information systems/communications performed by _____*(insert summary of any findings of any Command specific threat assessments)*

Based upon previous NSTISSC findings, the threat of any successful TEMPEST attack on *Command* information systems located in the continental United States is adjudged to be extremely low.

(If all or portions of Command System/Network information processing equipment is located overseas or in high threat areas, insert latest assessment of TEMPEST threat in such areas. See National Security Telecommunications and Information Systems Instruction (NSTISSI) No. 7000, Annex A(C) and the Composite Threat List (CTL) published on a semiannual basis by the State Department's Office of Diplomatic Security).

The threat of terrorist attack on *Command* facilities must be rated as *high/moderate,* based upon the bombing in Saudi-Arabia, the Oklahoma City bombing, the attack on the World Trade Center, threats issued against U.S. Government installations subsequent to the recent U.S. Embassy bombings in Africa, and the environment in which *Command System/Network* facilities operate with relation to the threat.

(The level of this threat with relation to the Command System/Network will be based upon an assessment of the threat in relation to the processing environment of the System/Network)

Because of the environment within which the *Command System/Network* resources operate, the threats posed by riot, civil disturbance and vandalism are considered to be *high/moderate/low/minimal*.

The final threats to the security of the *Command System/Network* that must be considered are:

- Damage by fire and water,
- Natural disasters (e.g., storms, floods, earthquakes),
- Power failure,
- Hardware failure (including air conditioning),
- Communication system failure.

2.3.2 Threat Environment and Single Points of Failure

There are *one/two/...n* potential single points of failure of substantially all of the system capabilities. The first involves the total loss of power to the *Command HQ/other* building*(s)*. The commercial power system supply to *this/these* building*(s)* is *extremely reliable/reliable/unreliable*. Because of *the richly interconnected power grid of the* _____

Power Company in _____ and the surrounding area, the commercial power supply is only likely to be disrupted for any extensive period of time by a major natural disaster such as an earthquake or the direct impact of hurricanes or tornadoes, the likelihood of the occurrence of any of these natural disasters is adjudged to be very low./other statements concerning the reliability of the commercial power to critical system components and the likelihood of natural disasters that would affect the commercial power supply.

The *other/second* potential single point of failure involves the destruction of all or substantially all of the equipment located in the _____ by fire, terrorist attack, sabotage, or natural disaster. Since the fire resistance of the _____ building*(s)* is *high/medium/low* and the fire protection and suppression facilities available to the buildings *meets/fail to meet* fire code requirements, the risk of substantial destruction as a result of fire of the equipment located in the ____ is deemed to be *high/medium/low*. In the light of the *strong* physical access controls and the *stringent* personnel clearance procedures governing building access, the risk of destruction of this equipment through terrorist attack or sabotage is deemed to be *high/moderate/low*. Based upon the *substantial/moderately high grade/insubstantial* construction of the _____ building(s) and the *high/moderate/low* likelihood of the occurrence of direct impact of a hurricane or tornado or of an earthquake of significant magnitude in the local area, destruction of this equipment as a result of natural disaster is deemed to be *high/moderate/low*.

The *n* potential point of failure involves *(Insert similar discussion of threats to system nodes that constitute single points of failure to the system*

For more examples, see Examples_Addendum.

Type your text here.

3.0 SYSTEM ARCHITECTURAL DESCRIPTION

This section is blank; it is a title.

For additional information, see DITSCAP Application Document, Section C3.3.4.

(Note: Most of the text of the examples incorporated in the body of this document are based upon, and intended to be consistent with, the general system description of a hypothetical DoD secret-level information system and network. The example of a detailed system architecture contained in this section is based upon a sanitized version of a previously developed actual system. It is included to provide an example of the level of detail and the recommended coverage of a system to be included in this section.

3.1 Hardware

Describe the target hardware and its function. If the equipment employed in the system that is the subject of the SSAA is voluminous, a general description of the amounts and types of equipment employed can be included in this section and a detailed equipment list incorporated as an appendix. If the development effort involves a change of existing hardware, identify the specific hardware components being changed. Additionally, describe the communications security (COMSEC) and TEMPEST features of the system and operation.

Based upon National Security Telecommunications and Information Systems Committee Instruction (NSTISSI) 7000 and related National Security Telecommunications and. Information Systems Committee (NSTISSIC) memorandums no TEMPEST countermeasures are required for these COMMAND SYSTEM/NETWORK equipment or facilities.

For additional information, see DITSCAP Application Document, Section C3.3.4.2.1.

Example:

The COMMAND classified LAN hardware consists of several workstations. There are seven workstations in Room X, eight workstations and 1 server in Room X, 16 workstations in Room X, and 7 workstations in Room X. All workstations consist of the CPU, monitor, keyboard, and mouse.

Workstations vary in manufactures and CPU type. In Room X there are three Hewlett Packard (HP) Vanguard series (all on the COMMAND network) and four Advanced Data Systems (ADS) (one Unclassified, three Classified). In Room X, there are four SUN SPARCstations (all Unclassified), one ADS (Unclassified), two Dell Poweredge 4200 series (Unclassified database server and web server) and a HP K Class 9000 serving as the Unclassified server. Room X consists of nine SUN SPARCstations (seven Unclassified and two Classified), one of which serves as the Classified server, one HP Apollo series (Unclassified), two ADS (Unclassified), one HP 725 series (Classified), and one CTX (Unclassified). In Room X there are seven workstations. Of these workstations, six are SUN SPARCstations. The seventh workstation is a Dell Poweredge 2200. In Room X there are two ADS workstations. One is on the COMMAND network and the other is on the Classified LAN. Other hardware components for the COMMAND classified LAN consists of Cisco AGST router, KG 194A, EAZY Serial Port, Access T DSU/CSU, HP LaserJet printers, Tektronix printers and Uninterruptable Power Supply. A complete inventory of the COMMAND classified LAN hardware items is located at Address.

For more examples, see Examples_Addendum.

Type your text here.

3.2 SOFTWARE

Describe the operating system(s), database management system(s), and applications. Describe the features of any security packages. Describe the target software and its intended use. Identify whether the software is COTS, GOTS, or on the EPL. This includes manufacturer supplied software, other COTS software, and all program generated applications software.

For additional information, see DITSCAP Application Document, Section C3.3.4.2.2.

Example:

The COMMAND classified LAN software consists of operating systems and applications resident on the workstations. This operating system is certified at the C-2 level of trust according to the National Computer Security Center (CSC) Trusted Computer System Evaluation Criteria. The SUN SPARCstations use the Solaris 2.5.1 operating system. The Advanced Data System, Dell and HP systems use the Microsoft Windows NT operating system. Varieties of general office applications are available to the various COMMAND classified LAN systems. A majority of these applications is resident on the COMMAND classified LAN server. See Address for a complete inventory of the COMMAND classified LAN software.

For more examples, see Examples_Addendum.

Type your text here.

3.3 FIRMWARE

Describe the firmware used and whether it is a standard commercial product, unique, or on the EPL. Describe the software that is stored permanently in a hardware devise that allows reading and executing the software, but not writing or modifying it.

For additional information, see DITSCAP Application Document, Section C3.3.4.2.3.

Example:

The COMMAND classified LAN hardware includes only standard manufacturer provided COTS firmware.

For more examples, see Examples_Addendum.

Type your text here.

3.4 SYSTEM INTERFACES AND EXTERNAL CONNECTIONS

Describe the system's external interfaces, including the purpose of each external interface and the relationship between the interface and the system. Describe the significant features of the communications layout, including a high level diagram of the communications links and encryption techniques connecting the components of the system, associated data communications, and networks.

For additional information, see DITSCAP Application Document, Section C3.3.4.2.4.

Example:

The *COMMAND SYSTEM/NETWORK* LAN internal architecture and the *COMMAND SYSTEM/NETWORK* 'S external interfaces are depicted in Figure 3.4. SIPRNET is not connected to any other *COMMAND* classified system. A KG-194A cryptographic device encrypts the external link to the SIPRNET. The external link to the *COMMAND* WAN is also depicted in Figure 3.4. An NSA approved NES encryption device encrypts the external link to the *COMMAND* WAN. The external users of the *COMMAND SYSTEM/NETWORK* from the SIPRNET are members of the *COMMAND* community of interest (the DoD, Services, CINCs, Joint Staff, and DoD Agency personnel) who have a SIPRNET account and an account on the *COMMAND SYSTEM/NETWORK*. External users of the *COMMAND SYSTEM/NETWORK* from *COMMAND* WAN are *COMMAND* personnel who have an account on one of the other systems connected to the *COMMAND* WAN and an account on the *COMMAND SYSTEM/NETWORK*. *The fiber optic link between Building A and Building B is contained within a protected distribution system (PDS) that meets all applicable COMSEC requirements.*

> *(Insert Figure - If existing system documentation contains a suitable figure or diagram it can be used. If not a figure should be created that shows the described network components and interfaces.)*

For more examples, see Examples_Addendum.

Type your text here.

3.5 DATA FLOW (INCLUDING DATA FLOW DIAGRAMS)

Describe the system's internal interfaces and data flows, including the types of data and the general methods for data transmission. Describe the specific transmission media or interfaces to other systems. The descriptions must include diagrams or text to explain the flow of critical information from one component to another.

For additional information, see DITSCAP Application Document, Section C3.3.4.2.5.

Example:

Figure 3.5 shows the COMMAND classified data flow. The primary correspondents, the US Government agencies and facilities, and the military community users who possess a SIPRNET or an account on a system connected to the COMMAND WAN, or an account on the COMMAND SYSTEM/NETWORK, are provided access to the COMMAND SYSTEM/NETWORK. COMMAND SYSTEM/NETWORK users are provided access to information resources on the SIPRNET or on the COMMAND WAN through these external system interfaces. As shown, e-mail and attachments classified at secret or below may transition both directions across this interface.

(Insert Figure)

For more examples, see Examples_Addendum.

Type your text here.

3.6 DOD TECHNICAL ARCHITECTURE FRAMEWORK FOR INFORMATION MANAGEMENT (TAFIM) DOD GOAL SECURITY ARCHITECTURE (DGSA)

Compare the significant features of the system with the DGSA. Include a diagram of the relationship of the system architecture to the DGSA. Systems being designed with architecture inconsistent with the DGSA must be evaluated to ensure that sufficient justification exists for not complying with the DGSA's architectural recommendations.

For additional information, see DITSCAP Application Document, Section C3.3.4.2.6.

Example:

For examples, see Examples_Addendum.

Type your text here.

3.7 ACCREDITATION BOUNDARY

Describe the boundary of the system. The description must include diagrams or text to clearly delineate which components are to be evaluated as part of the C&A task and which are not included. All components included must be described in the system description. Elements outside the accreditation boundary must be included in the section on external interfaces.

For additional information, see DITSCAP Application Document, Section C3.3.4.2.7.

Example:

The boundary of the COMMAND SYSTEM/NETWORK accreditation includes the COMMAND SYSTEM/NETWORK communications and computer equipment located within Buildings A and B at Fort ABC. The information system comprising the hardware and software identified above constitute the entire COMMAND SYSTEM/NETWORK. The boundary extends from the COMMAND SYSTEM/NETWORK workstations and associated peripherals through the KG 194A and Channel Service Unit/Data Service Unit (CSU/DSU) to the SIPRNET and through the NES encryption device to the COMMAND WAN. Both the SIPRNET and the COMMAND WAN also operate in the system high Secret mode of operation and are separately accredited to operate at that level.

See Figure 3.7: COMMAND SYSTEM/NETWORK Accreditation Boundary

For more examples, see Examples_Addendum.

Type your text here.

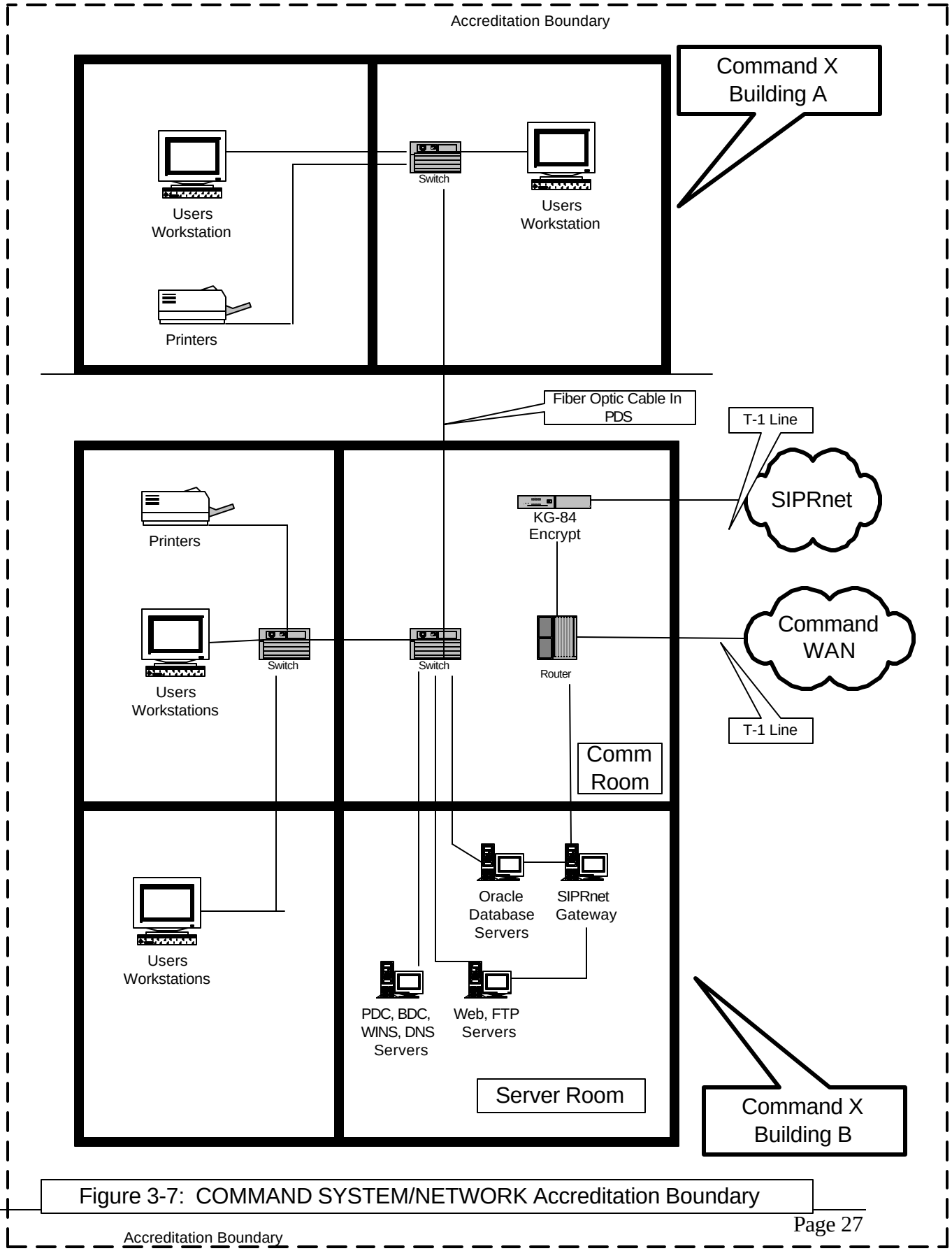

Figure 3-7: COMMAND SYSTEM/NETWORK Accreditation Boundary

4.0 ITSEC SYSTEM CLASS

This section is blank; it is a title.

For more information, see DITSCAP Application Document, Section AP2.1.

4.1 INTERFACING MODE

Determine the risk to other operations, data, or systems if a problem were to occur with your system's operation or data. The interactions between systems may be either physical or logical relationships. The interfacing mode can be benign, passive, or active.

For more information, see DITSCAP Application Document, Section AP2.2.2.

Example:

The interfacing mode profile for the COMMAND SYSTEM/NETWORK is "Active," which implies direct interaction with both physical and logical relationships.

For more examples, see Examples_Addendum.

Type your text here.

4.2 PROCESSING MODE

Determine how the system processes, transmits, and stores data. The processing mode can be dedicated, compartmented, system high, or multi-level.

For more information, see DITSCAP Application Document, Section AP2.2.3.

Example:

The processing mode of the COMMAND SYSTEM/NETWORK is system high at the Secret level.

For more examples, see Examples_Addendum.

Type your text here.

4.3 ATTRIBUTION MODE

Determine the degree to which the system can attribute the processing, transmitting, or storing of data to a specific user or process. The attribution mode can be none, rudimentary, selected, or comprehensive.

For more information, see DITSCAP Application Document, Section AP2.2.4.

Example:

For the COMMAND SYSTEM/NETWORK and its workstation elements, the attribution mode is "Selected." Some processing, transmission, storage, or data carries the ability to attribute them to users or processes.

For more examples, see Examples_Addendum.

Type your text here.

4.4 MISSION-RELIANCE FACTOR

Determine the degree to which the mission is dependent on the system's operation, infrastructure, or data. The mission-reliance factor can be none, cursory, partial, or total.

For more information, see DITSCAP Application Document, Section AP2.2.5.

Example:

Since the COMMAND mission can in large measure continue to be performed, at least for a reasonable period of time, without the availability of the COMMAND SYSTEM/NETWORK , the mission-reliance factor of the system is partial.

For more examples, see Examples_Addendum.

Type your text here.

4.5 ACCESSIBILITY FACTOR

Determine how accessible the system must be to as it relates to security risks. The accessibility factor can be reasonable, soon, ASAP, or immediate.

For more information, see DITSCAP Application Document, Section AP2.2.6.

Example:

The appropriate accessibility factor profile choice for the COMMAND SYSTEM/NETWORK is "Immediate." The "Immediate" profile means that the specific aspect, i.e., the operation, data, infrastructure, or system, must be available immediately to avoid operational impacts.

For more examples, see Examples_Addendum.

Type your text here.

4.6 ACCURACY FACTOR

Determine how accurate the system must be as it relates to security risks. The accuracy factor can be not applicable, approximate, or exact.

For more information, see DITSCAP Application Document, Section AP2.2.7.

Example:

The accuracy factor that is applied to the COMMAND SYSTEM/NETWORK is "Exact." This factor means that the degree of integrity for a specific aspect, i.e., the operation, data, infrastructure, or system, must be exact in order to avoid operational impacts.

For more examples, see Examples_Addendum.

Type your text here.

4.7 INFORMATION CATEGORIES

Determine the information category for the system. If more than one category of information is involved in a system, the system must satisfy all the security requirements of each of the information categories. The information categories can be unclassified, sensitive information, collateral classified, or compartmented/special access classified.

For more information, see DITSCAP Application Document, Section AP2.2.8.

Example:

All elements of the COMMAND SYSTEM/NETWORK are on the "Collateral Classified" ITSEC System Class category. Contained within this category are appropriate subcategories of privacy act, financially sensitive, proprietary, and administrative data.

For more examples, see Examples_Addendum.

Type your text here.

4.8 SYSTEM CLASS LEVEL

For more information, see DITSCAP Application Document, Section AP2.4.

Complete the system class chart.

Characteristic	Operation	Data	Infrastructure	System
Interfacing Mode				
Processing Mode				
Attribution Mode				
Mission-Reliance Factor				
Accessibility Factor				
Accuracy Factor				
Information Categories				

Determine the assigned weight based on the information in the system class chart.

Characteristic	Selection Alternatives	Assigned Weight
Interfacing Mode	Benign (w=1) Passive (w=3) Active (w=7)	
Processing Mode	Dedicated (w=1) Compartmented Level (w=2) System High (w=5) Multi-level (w=8)	
Attribution Mode	None (w=1) Rudimentary (w=2) Selected (w=4) Comprehensive (w=6)	

Characteristic	Selection Alternatives	Assigned Weight
Mission-Reliance Factor	None (w=0) Cursory (w=1) Partial (w=3) Total (w=7)	
Accessibility Factor	Reasonable (w=1) Soon (w=2) ASAP (w=4) Immediate (w=7)	
Accuracy Factor	Not-applicable (w=0) Approximate (w=2) Exact (w=5)	
Information Categories	Unclassified (w=0) Sensitive (w=2) Collateral Classified (w= 5) Compartmented/Special Access Classified (w=7)	
Total of all weights.		

Type your text here.

4.9 CERTIFICATION ANALYSIS LEVEL

Determine the system class/certification level using the following chart.

Certification Level	Weight
Level l	Weighing factors are < 17
Level 2	Weighing factors are 13 - 26
Level 3	Weighing factors are 20 - 37
Level 4	Weighing factors are 30 - 47

The combined weighing factors of COMMAND SYSTEM/NETWORK have been determined to be 30. Therefore the Certification Level for the system is Level 3.

Type your text here.

5.0 SYSTEM SECURITY REQUIREMENTS

This section is blank; it is a title.

For more information, see DITSCAP Application Document, Section C3.3.5

5.1 National/DOD Security Requirements

Determine the security instructions or directives applicable to the system. In most cases, this will include national level directives, OMB Circulars A-123 and OMB A-130, and DoD directives. Each service or COMMAND may also have directives that dictate security requirements. All the directives that will impact the user should be identified. Many systems are also required to meet the requirements of the Trusted Computer Security Evaluation Criteria (TCSEC).

Example:

The system security requirements that govern the COMMAND are derived from public law, executive order, and regulations of designated agencies of the Executive Branch of the U.S. Government. Six requirements are of special significance to the COMMAND SYSTEM/NETWORK.

National Security Decision Directive 145 (NSDD 145). The National Policy on Telecommunications and Automated Information Systems Security, September 1984, later revised and reissued in 1990 as National Security Directive 42, mandates the protection of both classified and unclassified sensitive information processed, stored, and transmitted by SIPRNET. NSDD 145 requires the COMMAND SYSTEM/NETWORK to be as secure as necessary to prevent access by unauthorized individuals.

Public Law 100-235, known as the Computer Security Act of 1987, requires that every U.S. Government computer system, including the COMMAND's, that processes sensitive information, to have a customized computer security plan for the system's management and use. This law also requires that such system users receive periodic training in computer security.

Executive Order 12958, Classified National Security Information, signed 17 April 1995 to update Executive Order 12356, prescribes a uniform system for classifying, safeguarding, and declassifying national security information. The COMMAND SYSTEM/NETWORK is to follow the prescribed actions of this Executive Order.

Office of Management and Budge (OMB) Circular A-130, Management of Federal Information Resources, 8 February 1996, requires that computer systems, including the COMMAND, provide a level of security proportional with the sensitivity of the information, the risk of its unauthorized access, and the harm that could result from improper access. A-130 additionally requires that a security program be established to safeguard the sensitive information that the system processes.

Department of Defense Directive 5200.28, Security Requirements for Automated Information Systems, 21 March 1988, provides mandatory minimum-security requirements that apply to the COMMAND.

Department of Defense Information Technology Security Certification and Accreditation Process (DITSCAP) 5200.40, establishes a standard process, set of activities, general task descriptions, and a management structure to certify and accredit information technology systems that will maintain the security posture of DII. This guidance prescribes the methodology to be used in the development of the SSAA.

For more examples, see Examples_Addendum.

Type your text here.

5.2 GOVERNING SECURITY REQUISITES

Determine the requirements stipulated by local agencies and the Designated Approving Authority (DAA). Contact the DAA and user representative to determine if they have any additional security requirements.

For additional information, see DITSCAP Application Document, Section C3.3.6.2.3.

Example:

COMMAND Instruction XX.2, Automatic Data Processing, Information Systems Security Program, July 1996, prescribes security requirements for COMMAND automated information systems, including those connected to the COMMAND WAN. The policies outlined in this document provide a basis that COMMAND uses to develop its principles. It is DoD policy that classified and sensitive unclassified information is to be safeguarded at all times. Safeguards are applied such that only authorized persons access the protected information and used only for intended purposes. Classified and sensitive information is to retain content integrity and is to be marked properly. Information is to be safeguarded against sabotage, tampering, loss, denial of service, espionage, fraud, misappropriation, misuse, release to unauthorized persons, and destruction; it shall be available when needed. Personnel, physical, administrative, and technical controls are to be applied to information systems to furnish necessary protection. The governing DoD Directive 5220.28-STD and COMMAND security instructions require the employment of a mix of safeguards to ensure the COMMAND SYSTEM/NETWORK meets the defined set of minimum requirements. The DISN minimum requirements, which govern the security afforded to the COMMAND WAN, are defined below.

For more examples, see Examples_Addendum.

Type your text here.

5.3 DATA SECURITY REQUIREMENTS

Determine the type of data processed by the system. The type of data may require additional protections. Contact the data owner or organizations that have access to the system or share data with the system to determine their security requirements.

For additional information, see DITSCAP Application Document, Section C3.3.6.2.3.

Example:

Safeguards are employed by the COMMAND SYSTEM/NETWORK to detect and minimize unauthorized disclosure, modification, or destruction of data. Such safeguards include user authentication for logging onto a system, and access control once logged on. Such safeguards ensure that the COMMAND SYSTEM/NETWORK information is protected from the potentially destructive impact of human error as well as malicious logic and unauthorized modification of hardware, software, or data. Automated or manual procedures are employed to mark or accurately reflect the sensitivity and classification of information processed by COMMAND SYSTEM/NETWORK. All output is protected at the highest classification level of information processed, stored, or transmitted by the COMMAND SYSTEM/NETWORK. Prior to release, COMMAND SYSTEM/NETWORK information is subject to review by an authorized person to ensure automated markings are accurate and unmarked output is manually applied as appropriate. COMMAND SYSTEM/NETWORK media is stored, marked, reproduced, destroyed, or otherwise controlled, sufficiently to ensure the protection of classified or unclassified, but sensitive data that may be stored on the media.

For more examples, see Examples_Addendum.

Type your text here.

5.4 SECURITY CONOPS

Describe the security concept of operations (CONOPS) including system input, system processing, final outputs, security controls and interactions, and connections with external systems. Include diagrams, maps, pictures, and tables in the security CONOPS. If a system CONOPS is available, a summary of the security portions of the CONOPS should be reviewed and added to the SSAA. If a security CONOPS, Trusted Facility Manual (TFM), or Security Features Users Guide (SFUG) is available, a summary of that information should be added to the SSAA. The security CONOPS, TFM, or SFUG document may be added as an appendix or listed as a reference.

For additional information, see DITSCAP Application Document, Section C3.3.6.2.4.

Example:

This security concept of operations (SCONOPS) provides information about the secure operations of the Agency classified LAN. The S-CONOPS describes the mission that the Agency classified LAN supports, the purpose for the Agency classified LAN, the administration and maintenance of the system, and the ways the Agency classified LAN security policy is implemented.

For more examples, see Examples_Addendum.

Type your text here.

5.4 SECURITY POLICY

Describe the security concept of operations (CONOPS) including system input, system processing, final outputs, security controls and interactions, and connections with external systems. Include diagrams, maps, pictures, and tables in the security CONOPS. If a system CONOPS is available, a summary of the security portions of the CONOPS should be reviewed and added to the SSAA. If a security CONOPS, Trusted Facility Manual (TFM), or Security Features Users Guide (SFUG) is available a summary of that information should be added to the SSAA. The security CONOPS, TFM, or SFUG document may be added as an appendix or listed as a reference.

For additional information, see DITSCAP Application Document, Section C3.3.6.2.4.

Example:

This security concept of operations (S-CONOPS) provides information about the secure operations of the COMMAND SYSTEM/NETWORK. The S-CONOPS describes the mission that the COMMAND SYSTEM/NETWORK supports, the purpose for COMMAND SYSTEM/NETWORK, the administration and maintenance of the system, and the ways the COMMAND SYSTEM/NETWORK security policy is implemented. (Insert summary of the S-CONOPS here or attach existing system S-CONOPS related documentation as an additional appendix and include a reference here.

For more examples, see Examples_Addendum.

Type your text here.

5.5 NETWORK CONNECTION RULES

Identify any additional requirements incurred if the system is to be connected to any other network or system. These requirements and those of other systems that may be connected to the system or network must be added to the SSAA.

For additional information, see DITSCAP Application Document, Section C3.3.6.2.5.

Example:

The COMMAND connection policy is to ensure the prevention of unauthorized access to the COMMAND SYSTEM/NETWORK information via an external connection. The COMMAND SYSTEM/NETWORK shall employ only authorized and controlled external connectivity. Uncontrolled external connectivity significantly increases the vulnerability of COMMAND SYSTEM/NETWORK confidentiality, integrity, and availability. Periodically the COMMAND conducts unannounced vulnerability tests to verify the COMMAND SYSTEM/NETWORK architecture and report any external anomalies to the ISSO. Corrective actions shall be initiated immediately and reported to the testing office. The COMMAND SYSTEM/NETWORK has the capability to restrict external connection by control of TCP/IP communication protocol settings on the COMMAND SYSTEM/NETWORK routers. Only approved, certified, and accredited external connections are authorized. The COMMAND SYSTEM/NETWORK Security Administrator shall manage all access controls (e.g., configuration tables, host tables, and passwords) pertaining to network and communication components, such as routers). Any additional external connections are subject to the prior review and approval by the COMMAND CONFIGURATION CONTROL BOARD.

For more examples, see Examples_Addendum.

Type your text here.

5.6 CONFIGURATION AND CHANGE MANAGEMENT REQUIREMENTS

Determine if there are any additional requirements based on the configuration management plan. These instructions may be described in a configuration management policy of Configuration Management Review Board charter. The documents should be reviewed to determine if any additional requirements exist that should be evaluated.

For additional information, see DITSCAP Application Document, Section C3.3.6.2.6.

Example:

The COMMAND CONFIGURATION CONTROL BOARD must evaluate the impact on security of all changes (hardware, software, and firmware) to the system and any proposed additional system or network connections.

For more examples, see Examples_Addendum.

Type your text here.

5.7 REACCREDITATION REQUIREMENTS

Determine if there are unique organizational requirements related to the reaccreditation or reaffirmation of the approval to operate the system.

For additional information, see DITSCAP Application Document, Section C3.3.6.2.7.

Example:

Information processing assets are reaccredited at least every 3 years or when a major change has been made that impacts security. The level of effort required for recertification and reaccreditation action depends on the scope of the change to the security environment. Review of configuration management activities and the current environment by the DAA and certifying authority determines the actions required for reaccreditation. Reaccreditation may include the same steps accomplished for the original accreditation; however, portions of the security documentation, which remains valid, will not need to be redone. The following is a representative (not all inclusive) example of events that may impact security and could require reaccreditation action. The ISSM/ISSO must submit a request for reaccreditation under the conditions that follow:

- *A change in criticality or sensitivity level of the information processed.*
- *A breach of security or violation of system integrity which reveals a flaw in security design, system security management, policy, or procedure.*
- *A change in the threat environment impacting overall system risks.*
- *A change in the system security mode of operation.*
- *A change in the operating system, security software, or hardware that affects the accredited security countermeasure implementation.*

For more examples, see Examples_Addendum.

Type your text here.

5.8 REQUIREMENTS TRACEABILITY MATRIX

Analyze the directives and security requisites to determine the system security requirements. Enter the security requirements into a requirements traceability matrix (RTM). The following is a sample RTM.

For additional information, see DITSCAP Application Document, Section C3.3.6.2.8.

Req. No.	Requirement	Source	Related Req.	Review				Comments
				I	D	T	O	
	Fundamental Computer Security Requirements							
F-1	Req. 1 – Security policy – There must be an explicit and well-defined security policy enforced by the system…	TCSEC Intro. p. 3 TNI 2.2.1	DOJ 2640.2C-14	X	X	X		See Req. F2 – F6
F-2	Req. 2 – Marking – Access control labels must be associated with objects…	TCSEC Intro. p. 3	TCSEC 2.2.1.1	X	X	X		See DAC. 1 – 6
	General Requirements							
G-1	Agencies must implement and maintain a program to assure that adequate security is provided for all agency information…	OMB A-130, App. III		X	X		X	

For more examples, see Examples_Addendum.

Type your text here.

6.0 ORGANIZATIONS AND RESOURCES

This section is blank; it is a title.

6.1 ORGANIZATIONS

Identify the organizations, individuals, and titles of the key authorities in the Certification and Accreditation (C&A) process.

For additional information, see DITSCAP Application Document, Section C3.3.7.2.1.

Example:

The organizations responsible for performing, or supporting, requirements and tasks contained in the COMMAND SYSTEM/NETWORK SSAA include COMMAND SYSTEM/NETWORK Information Systems staff, COMMAND Office of Information Security, COMMAND

SYSTEM/NETWORK Program Office, representative of the DAA, representative of the tester, and the supporting contractor(s). The Office of Information Security is responsible for ensuring that sponsors of an application system comply with the security policy and procedures for COMMAND SYSTEM/NETWORK. The COMMAND SYSTEM/NETWORK Program Office provides technical assistance on issues regarding application systems. Other COMMAND SYSTEM/NETWORK staff may be called upon to support the C&A as required.

For more examples, see Examples_Addendum.

Type your text here.

6.2 RESOURCES

Identify the resources required to conduct the C&A. If a contractor is involved or individuals from other government organizations are temporarily detailed to assist in the C&A process, funding requirements must be defined and included in the SSAA. The composition and size of the team will depend on the size and complexity of the system. The team must have members with composite expertise in the whole span of activities required, and who are independent of the system developer or project Program Manager.

For additional information, see DITSCAP Application Document, Section C3.3.7.2.2.

Example:

The PM, Office, employs a staff of COMMAND employees and contract personnel to prepare for system certification and accreditation and to execute the subsequent maintenance phase of accreditation. The COMMAND system and security engineers and administrators who operate and maintain the COMMAND classified LAN are educated professionals who meet the technical requirements imposed by the COMMAND for their positions. The PM, Office, provides the intellectual and material resources and management supervision to execute all elements of the certification and accreditation preparation phase. Other resources provided include computer and communication resources, office equipment, and general supplies. The specific areas of concern in this phase include risk management, certification test plan preparation, preliminary certification testing, and accreditation documentation preparation. The resources of the Office are adequate to support all efforts associated with the certification and accreditation of the COMMAND classified LAN.

For more examples, see Examples_Addendum.

Type your text here.

6.3 TRAINING

Describe the C&A training requirements, types of training, who is responsible for preparing and conducting the training, what equipment is required, and what training devices must be developed to conduct the training, if training is required. Funding for the training must be identified.

For additional information, see DITSCAP Application Document, Section C3.3.7.2.2.

Example:

The Chief, COMMAND Network Services Office has ensured the members of his Government staff are adequately trained to oversee and execute the preparatory COMMAND SYSTEM/NETWORK certification actions. The supporting contract staff contains expertise in all functional areas necessary to achieve and maintain system accreditation. The staff are trained and experienced in preparing and executing certification test plans. However, two days of training is required in the use of ABC test tool. The vendor provides this training at a cost of $300 per student. The staff of the COMMAND is likewise trained in all aspects of certification testing. The test team selected by the COMMAND receive specific information on the COMMAND SYSTEM/NETWORK from the SSAA and its appended Security Test and Evaluation (ST&E) Plan in advance of the actual certification test. The COMMAND ensures the test team understands the hardware, software, and communication components of COMMAND SYSTEM/NETWORK. Prior to executing the approved ST&E, specific training is provided on any technological features incorporated in the COMMAND SYSTEM/NETWORK structure not fully understood by the COMMAND SYSTEM/NETWORK staff.

For more examples, see Examples_Addendum.

Type your text here.

6.4 ROLES AND RESPONSIBILITIES

Identify the roles of the certification team and their responsibilities. The certification team may include individuals from many organizations.

For additional information, see DITSCAP Application Document, Section C3.3.7.2.3.

Example:

The primary assignments of team personnel are listed in Table 6-4. This table lists the contractor labor categories to be utilized and the personnel within those categories who are scheduled to perform the tasks as required under this delivery order. Key management, quality assurance, program and financial control, and support personnel were identified in Section 6.2 above.

All contractor personnel meet or exceed the requirements stated in the Personnel Qualifications of the prime contract. All staff resumes have been approved for work on this task. All of the contractor technical personnel assigned to this task have extensive experience in INFOSEC C&A and performance of tasks.

Ms. A, TM of this task, is responsible for the day-to-day operations of the task and the personnel assigned.

Assisting Ms. A are Mr. B, Test Director; Ms. C, test member; Ms. D, test member; Mr. E, DISA Observer; Senior INFOSEC Analysts Ms. F, Mr. G and Mr. H. Mr. B is responsible for the ST&E planning, procedures, conduct and test report. Ms. F is responsible for reviewing the SSAA, Security Test & Evaluation (ST&E) Test Plan, Procedures, Test Reports, and technical papers for their accuracy. Mr. G and Mr. H will provide expertise in the development of the COMMAND SYSTEM/NETWORK SSAA. Mr. G has been part of the DITSCAP development since its inception. Mr. H has extensive experience in the C&A of information systems and has recently successfully applied the DITSCAP process at the X U&S COMMAND. Mr. I and Mr. J, Senior Communications Security Engineers, will assist Mr. B with the security communications engineering and technical direction. In addition their expertise is required to recommend solutions to the most difficult communications problems in existing systems and in systems development. Mr. I and Mr. J have extensive experience in the XYZ Community as lead engineers in the XYZ SYSTEM ST&E. Ms. K, the Administrative Assistant Intermediate is key to the production of the number of documents required in this task.

To ensure the successful completion of this task, the TM has requested personnel experienced and knowledgeable in areas such as the COMMAND and DITSCAP objectives and a familiarity with large enterprise systems. Personnel will have knowledge of applicable security requirements and policies and shall have experience in the analysis of system security posture, performance of risk analyses, and preparation of policies, plans, and other documentation required to support the C&A of COMMAND systems and communications architecture. The C&A Team has experience in the Federal Government and Defense Community with both unclassified but sensitive and classified systems, possess a full understanding of National information security requirements; are qualified in the use of automated hardware platforms, software, and databases; and are qualified in the use of physical and automated security measures to provide oversight and technical assistance. All assigned work will be coordinated with the task manager, Ms. A, and the COMMAND Action Officer to ensure agreement on approach and results.

For more examples, see Examples_Addendum.

Type your text here.

6.5 OTHER SUPPORTING ORGANIZATIONS

Identify any other organizations or working groups that are supporting the C&A process.

Example:

Identify the characteristics within the organization what might effect the level of effort required for the C&A of the system.

For more examples, see Examples_Addendum.

Type your text here.

7.0 DITSCAP PLAN

This section is blank; it is a title.

7.1 TAILORING FACTORS

This section is blank; it is a title.

7.1.1 Programmatic Considerations

Programmatic considerations are the first group of tailoring factors that may influence the COMMAND SYSTEM/NETWORK accreditation process. This element of DITSCAP integrates the certification and accreditation activities with the COMMAND SYSTEM/NETWORK development, modification, and maintenance activities. Adjust the DITSCAP schedule to the program acquisition strategy and system lifecycle.

For additional information, see DITSCAP Application Document, Section C3.3.8.2.2.

Example:

The hardware and software components of the defined system are identified in Section 3. No plans to change, upgrade, or add to the current hardware or software components with the exception of the proposed future E-mail gateway to the COMMAND sensitive but unclassified WAN. The COMMAND SYSTEM/NETWORK primarily consists of commercial software and a limited number of hardware and software components. Only one unique software application

has been developed to integrate the various component software elements of the COMMAND SYSTEM/NETWORK.

For more examples, see Examples_Addendum.

Type your text here.

7.1.2 Security Environment

The security environment in which the COMMAND SYSTEM/NETWORK operates is a second tailoring factor that may influence the accreditation process. Identify any security requirements that might effect the level of effort required for the C&A process. The security requirements may include personnel, physical, administrative, procedural, operational, computer, network, and communications security components.

Example:

Section 5 of this SSAA defines the COMMAND SYSTEM/NETWORK system security requirements. These requirements include personnel, physical, administrative, procedural, operational, computer, network, and communications security components. The COMMAND SYSTEM/NETWORK security environment is not complicated. All users are cleared to the SECRET level, the maximum classification of system operations, and have signed nondisclosure statements. Need-to-know controls meet System High mode operation requirements. Physical security of the N COMMAND SYSTEM/NETWORK rooms where classified processing occurs meets COMMAND standards. Access controls adhere to published National, DoD and COMMAND guidance. All external communications are encrypted by a NSA provided or approved device and are transmitted over Secret communications backbones, SIPRNET, and the COMMAND WAN.

For more examples, see Examples_Addendum.

Type your text here.

7.1.3 IT System Characteristics

Information system characteristics comprise the third area of the tailoring factors. Identify the information technology characteristics of the system that might influence the level of effort required for the C&A process.

Example:

The COMMAND SYSTEM/NETWORK employs five commercial hardware platforms: Hewlett Packard, SUN, Dell, American Computing Systems, and Advanced Data Systems. Resident on these platforms are two common operating systems, Windows NT, and Solaris. The single Database Management System used is Oracle, Version n.n. Most of the software applications used are universally available commercial programs. Communications connectivity involves well-known and understood components such as CISCO routers, Ethernet switches, and the NSA KG-194 and NSA approved NES encryption devices. No unusual, experimental, or new model components complicate the COMMAND SYSTEM/NETWORK information system environment.

For more examples, see Examples_Addendum.

Type your text here.

7.1.4 Reuse of Previously Approved Solutions

Identify any previous approved solutions that may effect the level of effort required for the C&A process.

Example:

Reuse of previously approved solutions is a tailoring factor not applicable to COMMAND SYSTEM/NETWORK. No security features have been approved previously for use with the COMMAND SYSTEM/NETWORK.

For more examples, see Examples_Addendum.

Type your text here.

7.2 TASKS AND MILESTONES

List the security-related tasks and milestones for the system. The list should include detailed information about the activity, schedule, estimated duration of the activity, responsibility for the activity, and completion criteria.

For additional information, see DITSCAP Application Document, Section C3.3.8.2.4.

Example:

The COMMAND SYSTEM/NETWORK C&A actions will start on or about May 1999 to coincide with the planned system upgrade from Windows NT 3.51 to NT 4.0. DITSCAP phase I is scheduled to start as the system modifications begin. Phase 2 will follow immediately. Phase 3 will begin as soon as the system integration and acceptance testing is completed.

For more examples, see Examples_Addendum.

Type your text here.

7.3 SCHEDULE SUMMARY

List, in time order, the security activities associated with the system. A Gant chart may be added to clarify the schedule.

For additional information, see DITSCAP Application Document, Section C3.3.8.2.4.

Example:

The schedule of essential events pertaining to the COMMAND SYSTEM/NETWORK certification and accreditation is presented below.

Event	***Date***
Request for Certification Test by the COMMAND	*March 99*
Phase I commences	*1 May 99*
Phase I negotiations	*26 May 99*
Phase I SSAA complete	*15 June 99*
Phase 2 commences	*16 June 99*
Phase 2 complete	*15 July 99*
Phase 3 commences	*16 July 99*
ST&E	*10 August 99*
Phase 3 complete	*30 August 99*
Updated SSAA forwarded to PM, DAA, CA and User Rep.	*30 August 99*
DAA review of certification findings	*1 – 20 September 99*
DAA issues final accredition	*25 September 99*

For more examples, see Examples_Addendum.

Type your text here.

7.4 LEVEL OF EFFORT

Define the level of certification effort, as determined in Section 4.

For additional information, see DITSCAP Application Document, Section C3.3.8.2.4.

Example:

The level of certification effort, as determined in Section 4 above, is level 3, Detailed Analysis, which is described in the DITSCAP Application Document as:

> *"Level 3 requires completion of the minimal security checklist and more in-depth, independant analysis as defined in the Verification and Validation phases."*

For more examples, see Examples_Addendum.

Type your text here.

7.5 ROLES AND RESPONSIBILITIES

This section to be deleted. See section 6.4.

APPENDIX A – ACRONYM LIST

ASAP	As soon as possible
CA	Certification Authority
C&A	Certification and Accreditation
CCB	Change Control Board
CDR	Critical Design Review
CM	Configuration Management
COMPUSEC	Computer Security
COMSEC	Communications Security
CONOPS	Concept of Operations
COTS	Commercial Off-The-Shelf
CRLCMP	Computer Resources Life-Cycle Management Plan
CRMP	Computer Resource Management Plan
CRR	Certification Requirements Review
DAA	Designated Approving Authority
DAC	Discretionary Access Controls
DCID	Director of Central Intelligence Directive
DGSA	DoD Goal Security Architecture
DII	Defense Information Infrastructure
DITSCAP	DoD Information Technology Security Certification and Accreditation Process
DISN	Defense Information System Network
DISSP	Defense Wide Information Systems Security Program
DODIIS	Department of Defense Intelligence Information System
DoD	Department of Defense
DT&E	Developmental Test and Evaluation
EPL	Evaluated Product List
ESI	Extremely Sensitive Information
EPROM	Erasable Programmable Read Only Memory
ERTZ	Electromagnetic Radiation TEMPEST Zone
EMSEC	Emissions Security
FCA	Functional Configuration Audit
FIPS	Federal Information Processing Standard
FIRMR	Federal Information Resources Management Regulation
GOTS	Government Off-The-Shelf
I&A	Identification and Authentication
IASE	Information Assurance Support Environment
IATO	Interim Approval To Operate
INFOSEC	Information Systems Security
IOT&E	Initial Operational Test and Evaluation
ISSO	Information Systems Security Officer
IT	Information Technology
ITSEC	Information Technology Security
IV&V	Independent Verification and Validation
JTA	Joint Technical Architecture

LAN	Local Area Network
LCM	Life Cycle Management
MA	Maintenance Authority
MAC	Mandatory Access Controls
MDA	Milestone Decision Authority
MILDEP	Military Deputy
MIL-STD	Military Standard
MLS	Multi-Level Security
MNS	Mission Need Statement
MTBF	Mean Time Before Failure
MTTR	Mean Time To Return
NATO	North Atlantic Treaty Organization
NCSC	National Computer Security Center
NDI	Non-Developmental Item
NIST	National Institute of Standards and Technology
NSA	National Security Agency
NSTISSI	National Security Telecommunications and Information Systems Security Instruction
NSTISSIC	National Security Telecommunications and Information Systems Security Committee
NSTISSI 4009	National Telecommunications and Information Systems Security (INFOSEC) Glossary
NOFORN	No Foreign Dissemination
ORB	Operational Review Board
OMB	Office of Management and Budget
O/S	Operating System
OSD	Office of the Secretary of Defense
PCA	Physical Configuration Audit
PCS	Physical Control Space
PDR	Preliminary Design Review
PROM	Programmable Read Only Memory
PM	Project Manager
PUB. L.	Public Law
QA	Quality Assurance
RTM	Requirements Traceability Matrix
SAP	Special Access Program
SCI	Sensitive Compartmented Information
SCIF	Sensitive Compartmented Information Facility
SDM	System Decision Memorandum
SETA	Systems Engineering, Testing, and Analysis
SFUG	Security Features Users Guide
SIOP	Single Integrated Operations Plan
SIOP-ESI	Single Integrated Operations Plan - Extremely Sensitive Information
SPIRNet	Secret IP Router Network
SSAA	System Security Authorization Agreement

ST&E	Security Test and Evaluation
STD	Standard
TAFIM	Technical Architecture Framework for Information Management
TCB	Trusted Computing Base
TCSEC	Trusted Computer Security Evaluation Criteria
TEMPEST	Not an acronym
TFM	Trusted Facility Manual
TS	Top Secret
WAN	Wide Area Network

APPENDIX B – DEFINITIONS

The terms used in this document were selected from the NSTISSI 4009 (reference(i)) definitions when possible. Where new terms are used, the revised or new definitions will be submitted as changes to reference (i).

Accountability. Property that allows the ability to identify, verify, and trace system entities as well as changes in their status. Accountability is considered to include authenticity and non-repudiation.

Accreditation. Formal declaration by a DAA that an IT system is approved to operate in a particular security mode using a prescribed set of safeguards.

Architecture. The configuration of any equipment or interconnected system or subsystems of equipment that is used in the automatic acquisition, storage, manipulation, management, movement, control, display, switching, interchange, transmission, or reception of data or information; includes computers, ancillary equipment, and services, including support services and related resources.

Acquisition Organization. The Government organization responsible for developing a system.

Active System. A system connected directly to one or more other systems. Active systems are physically connected and have a logical relationship to other systems.

Assurance. Measure of confidence that the security features and architecture of an IT system accurately mediates and enforces the security policy.

Authenticity. The property that allows the ability to validate the claimed identity of a system entity.

Availability. The property of a resource being accessible and usable upon demand by an authorized user.

Audit. Independent review and examination of records and activities to assess the adequacy of system controls, to ensure compliance with established policies and operational procedures, and to recommend necessary changes in controls, policies, or procedures.

Benign System. A system that is not related to any other system. Benign systems are closed communities without physical connection or logical relationship to any other system. Benign systems are operated exclusive of one another and do not share users, information, or end processing with other systems.

Certification. Comprehensive evaluation of the technical and nontechnical security features of an IT system and other safeguards made in support of the accreditation process to establish the

extent to which a particular design and implementation meets a set of specified security requirements.

Certification Authority (CA). The official responsible for performing the comprehensive evaluation of the technical and nontechnical security features of an IT system and other safeguards made in support of the accreditation process to establish the extent to which a particular design and implementation meet a set of specified security requirements.

Compartmented Mode. INFOSEC mode of operation wherein each user with direct or indirect access to a system, its peripherals, remote terminals, or remote hosts has all the following: a. Valid security clearance for the most restricted information processed in the system; b. Formal access approval and signed non-disclosure agreements for that information to which a user is to have access; and c. Valid need-to-know for information to which a user is to have access.

Computing Environment. The total environment in which an automated information system, network, or a component operates. The environment includes physical, administrative, and personnel procedures as well as communication and networking relationships with other information systems.

COMSEC. Communications Security. Measures and controls established to deny unauthorized persons information derived from telecommunications and ensure the authenticity of such telecommunications. Note: Communications security includes cryptographic security, transmission security, emission security, and physical security of COMSEC material.

Confidentiality. The property that information is not made available or disclosed to unauthorized individuals, entities, or processes.

Configuration Control. Process of controlling modifications to an IT system's hardware, firmware, software, and documentation to ensure that the system is protected against improper modifications prior to, during, and after system implementation.

Configuration Management. Management of security features and assurances through control of changes made to hardware, firmware, software, documentation, test, test fixtures, and test documentation of an automated information system throughout the development and operational life of a system.

Configuration Manager. The individual or organization responsible for configuration control or configuration management.

Data Integrity. The attribute of data relating to the preservation of (1) its meaning and completeness; (2) the consistency of its representation(s); and (3) its correspondence to what it represents.

Dedicated Mode. IT security mode of operation in which each user, with direct or indirect access to the system, its peripherals, remote terminals, or remote hosts, has the following:

?? Valid security clearance for all information within the system.

?? Formal access approval and signed nondisclosure agreements for all the information stored and/or processed (including all compartments and/or special access programs).

?? Valid need-to-know for all information contained within the IT.

Defense Information Infrastructure (DII). The DII encompasses information transfer and processing resources, including information and data storage, manipulation, retrieval, and display. More specifically, the DII is the shared or interconnected system of computers, communications, data, applications, security, people, training, and other support structure, serving the DoD's local and worldwide information needs. The DII connects DoD mission support, command and control, and intelligence computers and users through voice, data, imagery, video, and multimedia services, and provides information processing and value-added services to subscribers over the DISN. Unique user data, information, and user applications software are not considered part of the DII.

Designated Approving Authority (DAA - Accreditor). Official with the authority to formally assume the responsibility for operating an IT system or network at an acceptable level of risk.

Developer. The organization that develops the information system.

DoD Information Technology Security Certification and Accreditation Process (DITSCAP). The standard DoD approach for identifying information security requirements, providing security solutions, and managing information system security activities.

Emissions Security (EMSEC). Protection resulting from measures taken to deny unauthorized persons information derived from intercept and analysis of compromising emanations from crypto-equipment or an information system.

Environment. The aggregate of external procedures, conditions, and objects that affect the development, operation, and maintenance of a system.

Evolutionary Program Strategies. Generally characterized by design, development, and deployment of a preliminary capability that includes provisions for the evolutionary addition of future functionality and changes, as requirements are further defined.

Governing Security Requisites. Those security requirements that must be addressed in all systems. These requirements are set by policy, directive, or common practice set, e.g., by Executive Order, OMB, Office of the Secretary of Defense, a military service or DoD agency. They are typically high-level. While their implementations will vary from case to case, these requisites are fundamental and must be addressed.

Grand Design Program Strategies. Characterized by acquisition, development, and deployment of the total functional capability in a single increment.

Incremental Program Strategies. Characterized by acquisition, development, and deployment of functionality through a number of clearly defined system "increments" that stand on their own.
Information Category. The term used to bound information and tie it to an information security policy.

Infrastructure-Centric. A security management approach that considers information systems and their computing environment as a single entity.

Information Integrity. The preservation of unaltered states as information is transferred through the system and between components.

Information Operations. Actions taken to affect adversary information and information systems while defending one's own information and information systems.

Information Security Policy. The aggregate of directives, regulations, rules, and practices that regulate how an organization manages, protects, and distributes information. For example, the information security policy for financial data processed on DoD systems can be contained in public law, executive orders, DoD directives and local regulations. The information security policy lists all the security requirements applicable to specific information.

Information System. Any telecommunication or computer-related equipment or interconnected system or subsystems of equipment that is used in the acquisition, storage, manipulation, management, movement, control, display, switching, interchange, transmission, or reception of voice and/or data; includes software, firmware, and hardware.

Information System Security Officer (ISSO). The person responsible to the DAA who ensures that an IT system is approved, operated, and maintained in accordance with the SSAA.

Information Technology (IT). The hardware, firmware, and software used as part of the information system to perform DoD information functions. This definition includes computers, telecommunications, automated information systems, and automatic data processing equipment. IT includes any assembly of computer hardware, software, and/or firmware configured to collect, create, communicate, compute, disseminate, process, store, and/or control data or information.

Information Technology Security (ITSEC). Protection and maintenance of confidentiality, integrity, availability, and accountability.

Integrator. The organization that integrates the information system components.

Integrity. The property that allows the preservation of known unaltered states between baseline certifications and allows information, access, and processing service to function according to specified expectations. It is composed of data integrity and system integrity.

Interim Approval To Operate. The system does not meet the requirements as stated in the SSAA, but mission criticality mandates the system become operational. The IATO is a temporary approval which may be issued for no more than a one-year period.

Legacy Information System. An operational information system that existed prior to the implementation of this process.

Maintainer. The organization that maintains the information system.

Maintenance Organization. The Government organization responsible for the maintenance of an IT system. (Although the actual organization performing maintenance on a system may be a contractor, the maintenance organization is the Government organization responsible for the maintenance.)

Mission Justification. The description of the operational capabilities required to perform an assigned mission. This includes a description of a system's capabilities, functions, interfaces, information processed, operational organizations supported, and the intended operational environment.

Multilevel Secure Mode. IT security mode of operation in which the following statements are satisfied concerning the users who have direct or indirect access to the system, its peripherals, remote terminals, or remote hosts:

?? Some users do not have a valid security clearance for all information processed in the IT.

?? All users have the proper security clearance and appropriate formal access approval for that information to which they have access.

?? All users have access only to information for which they have a valid need-to-know.

Mission. The assigned duties to be performed by a resource.

Non-Developmental Item (NDI). Any item that is available in the commercial marketplace; any previously developed item that is in use by a department or agency of the United States, a State or local government, or a foreign government with which the United States has a mutual defense cooperation agreement; any item described above that requires only minor modifications in order to meet the requirements of the procuring agency; or any item that is currently being produced that does not meet the requirements of definitions above, solely because the item is not yet in use or is not yet available in the commercial marketplace.

Operational Security (OPSEC). Process denying information to adversaries about capabilities and/or intentions by identifying, controlling, and protecting unclassified generic activities.

Other Program Strategies. Strategies intended to encompass variations and/or combinations of the Grand Design, Incremental, Evolutionary, or other program strategies.

Passive System. A system related indirectly to other systems. Passive systems may or may not have a physical connection to other systems, and their logical connection is controlled tightly.

Program Manager. The person ultimately responsible for the overall procurement, development, integration, modification, or operation and maintenance of the IT system.

Residual Risk. Portion of risk remaining after security measures have been applied.

Risk. A combination of the likelihood that a threat will occur, the likelihood that a threat occurrence will result in an adverse impact, and the severity of the resulting impact.

Risk Assessment. Process of analyzing threats to and vulnerabilities of an IT system, and the potential impact that the loss of information or capabilities of a system would have on a national security and using the analysis as a basis for identifying appropriate and cost-effective measures.

Risk Management. Process concerned with the identification, measurement, control, and minimization of security risks in IT systems.

Security. Measures and controls that ensure confidentiality, integrity, availability, and accountability of the information processed and stored by a computer.

Security Inspection. Examination of an IT system to determine compliance with security policy, procedures, and practices.

Security Process. The series of activities that monitor, evaluate, test, certify, accredit, and maintain the system accreditation throughout the system life-cycle.

Security Requirements. Types and levels of protection necessary for equipment, data, information, applications, and facilities to meet security policy.

Security Requirements Baseline. Description of the minimum requirements necessary for an IT to maintain an acceptable level of security.

Security Specification. Detailed description of the safeguards required to protect an IT system.

Security Test and Evaluation (ST&E). Examination and analysis of the safeguards required to protect an IT system, as they have been applied in an operational environment, to determine the security posture of that system.

Sensitive Information. Information the loss, misuse, or unauthorized access to or modification of which could adversely affect the national interest or the conduct of federal programs, or the privacy to which individuals are entitled under 5 U.S. C. Section 552a, but that has not been specifically authorized under criteria established by an Executive Order or an Act of Congress to be kept secret in the interest of national defense or foreign policy.

System. The set of interrelated components consisting of mission, environment, and architecture as a whole.

System Entity. A system subject (user or process) or object.

System Integrity. The attribute of a system when it performs its intended function in an unimpaired manner, free from deliberate or inadvertent unauthorized manipulation of the system.

System High Mode. IT security mode of operation in which each user with direct or indirect access to the IT, its peripherals, remote terminals, or remote hosts, has all of the following:

?? Valid security clearance for all information within an IT.

?? Formal access approval and signed nondisclosure agreements for all the information stored and/or processed (including all compartments, and special access programs).

?? Valid need-to-know for some of the information contained in the IT.

?? System Security Authorization Agreement (SSAA). The SSAA is a formal agreement among the DAA(s), the CA, the IT system user representative, and the program manager. It is used throughout the entire DITSCAP to guide actions, document decisions, specify ITSEC requirements, document certification tailoring and level-of-effort, identify potential solutions, and maintain operational systems security.

TEMPEST. Short name referring to investigation, study, and control of compromising emanations from IT equipment.

Threat. Capabilities, intentions, and attack methods of adversaries to exploit, or any circumstance or event with the potential to cause harm to, information or an information system.

Threat Assessment. Process of formally evaluating the degree of threat to an information system and describing the nature of the threat.

Trusted Computing Base (TCB). Totality of protection mechanisms within a computer system, including hardware, firmware, and software, the combination responsible for enforcing a security policy.

User. The individual or organization that operates or uses the resources of an information system.

User Representative. The individual or organization that represents the user or user community in the definition of information system requirements.

Utility. An element of the DII providing information services to DoD users. These services include Defense Information Systems Agency Megacenters, information processing, and wide area network communications services.

Validation. Determination of the correct implementation in the completed IT system with the security requirements and approach agreed upon by the users, acquisition authority, and DAA.

Verification. The process of determining the compliance of the evolving IT system specification, design, or code with the security requirements and approach agreed on by the users, acquisition authority, and DAA.

Vulnerability. Weakness in an information system, or cryptographic system, or components (e.g., system security procedures, hardware design, internal controls) that could be exploited.

Vulnerability Assessment. Systematic examination of an information system or product to determine the adequacy of security measures, identify security deficiencies, provide data from which to predict the effectiveness of proposed security measures, and confirm the adequacy of such measures after implementation.

APPENDIX C – REFERENCES

Office of Assistant Secretary of Defense Memorandum, The Defense Information Systems Security Program (DISSP), August 19, 1992.

DoD Directive 5200.28, "Security Requirements for Automated Information Systems (AISs)," March 21, 1988

Public Law 100-235, "Computer Security Act of 1987," January 8, 1988

Office of Management and Budget Circular No. A-130, "Management of Federal Information Resources," February 8, 1996

Director of Central Intelligence 1/16, "Security Policy on Intelligence Information in Automated Systems and Networks," March 14, 1988

DoD Directive 5220.22, "Industrial Security Program," November 1, 1986.

DoD Information Technology Security Certification and Accreditation (C&A) Process (DITSCAP), DoD Instruction 5200.40, 30 December 1997.

DoD Regulation 5000.2-R, Mandatory Procedures for Major Defense Programs (MDAPS) and Major Automated Information System (MAIS) Acquisition Programs, November 4, 1996.

National Information Systems Security (INFOSEC) Glossary, NSTISSI 4009, August 1997

An Introduction to Computer Security: The NIST Handbook, NIST Special Publication 800-12, October 1995.

The Certification and Accreditation Process Handbook for Certifiers, NCSC-TG-031, Draft, July 1996[1]

Management Accountability and Control, OMB A-123, June 21, 1995.

Accreditors Guideline, NCSC-TG-032, Draft July 1997[2]

Systems Engineering Management Guide, Defense Systems Management College, January 1990.

[1] Available from the DISA Information Systems Security Program Management Office, 701 Courthouse Road, Arlington, VA 22204-2199.

[2] Available from the DISA Information Systems Security Program Management Office, 701 Courthouse Road, Arlington, VA 22204-2199.

Computer Security Considerations in Federal Procurements: A Guide for Procurement Initiators, Contracting Officers, and Computer Security Officials, NIST Special Publication 800-4, March 1992.

Trusted Database Management System Interpretation, NCSC-TG-021, Version 1, April 1991.

Assessing Controlled Access Protection, NCSC-TG-028, Version 1, May 25, 1992.

A Guide to Understanding Design Documentation in Trusted Systems, NCSC-TG-007, Version 1, October 2, 1988.

Trusted network Interpretation Environments Guideline, NCSC-TG-011, Version 1, August 1, 1990.

A Guide to Understanding Trusted Recovery in Trusted Systems, NCSC-TG-022, Version 1, December 30, 1991.

Guideline for Life-cycle Validation, Verification, and Testing of Computer Software, FIPS Publication 101, June 6, 1983.

Software Verification and Validation: Its Role in Computer Assurance and Its Relationship with Software Project Management Standards, NIST Special Publication 500-165, September 1989.

Automated Tools for Testing Computer System Vulnerability, NIST Special Publication 800-6, December 1992.

A Guide to Understanding Audit in Trusted Systems, NCSC-TG-001, Version 2, June 1, 1988.

A Guide to Understanding Discretionary Access Control in Trusted Systems, NCSC-TG-003, Version 1, September 30, 1987.

A Guide to Understanding Identification and Authentication in Trusted Systems, NCSC-TG-017, Version 1, National Computer Security Center, September 1991.

A Guide to Understanding Object Reuse in Trusted Systems, NCSC-TG-018, Version 1, July 1, 1991.

Configuration Management Military Standard, MIL-STD-973, April 17, 1992.

A Guide to Understanding Configuration Management in Trusted Systems, NCSC-TG-006, Version 1, March 28, 1988.

A Guide to Understanding Trusted Distribution in Trusted Systems, NCSC-TG-008, Version 1, December 18, 1988.

Rating Maintenance Phase Program Documentation (NCSC-TG-013).

A Guide to Understanding Trusted Facility Management, NCSC-TG-015, Version 1, October 18, 1989.

Guidelines for Automatic Data Processing Physical and Risk Management, FIPS Publication 31, June 1974.

Guideline for Automatic Data Processing Risk Analysis, FIPS Publication 65, August 1, 1993.

Laboratory TEMPEST Test Standard, NSTISSAM TEMPEST/1-92.

Compromising Emanations Field Test Requirements, Electromagnetics, NSTISSAM TEMPEST/1-93, August 30, 1993.

Procedures for TEMPEST Zoning, NSTISSAM TEMPEST/2-92, December 30, 1992.

Guidelines for Facility Design and RED/BLACK Installation, NACSIM 5203, June 1, 1982.

Communications Security (COMSEC), DOD Directive C-5200.5, October 6, 1981.

Defense Special Security Communications: Security Criteria and Telecommunications Guidance, DOD-C5030.58-M, July 1978.

Communications Security (COMSEC) Monitoring, NTISSD 600, April 10, 1990.

INFOSEC Software Engineering Standards and Practices Manual, NSA DS-80, January 9, 1991.

Computer Security Guidelines for Implementing the Privacy Act of 1974, FIPS Publication 41, May 30, 1975.

Guidelines on Evaluation of Techniques for Automated Personal Identification, FIPS Publication 48, April 1, 1977.

Guidelines for Security of Computer Applications, FIPS Publication 73, June 30, 1980

Guideline on User Authentication Techniques for Computer Network Access Control, FIPS Publication 83, September 29, 1980.

Guidelines for ADP Contingency Planning, FIPS Publication 87, March 27, 1981.

Guideline for Computer Security Certification and Accreditation, FIPS Publication 102, September 27, 1988.

Password Usage, FIPS Publication 112, May 30, 1985.

Computer Data Authentication, FIPS Publication 113, May 30, 1985.

Defense Acquisition, DoD Directive 5000.1, March 15, 1996.

Memorandum on Information Management Definitions issued by the Assistant Secretary, 26 February 1994.

Subsection 552a of title 5, United States Code.

Department of Defense Technical Architecture Framework for Information Management (TAFIM), Volume 6, DoD Goal Security Architecture (DGSA), 30 April 1996[3]

[3] Available from the DISA Information Systems Security Program Management Office, 701 Courthouse Road, Arlington, VA 22204-2199.

APPENDIX D – SECURITY REQUIREMENTS AND/OR REQUIREMENTS TRACEABILITY MATRIX

APPENDIX E – SECURITY TEXT AND EVALUATION PLAN AND PROCEDURES

APPENDIX F – CERTIFICATION RESULTS

APPENDIX G – RISK ASSESSMENT RESULTS

APPENDIX H – CERTIFICATION AUTHORITY'S RECOMMENDATIONS

APPENDIX I – SYSTEM RULES OF BEHAVIOR

APPENDIX J – CONTINGENCY PLAN(S)

APPENDIX K – SECURITY AWARENESS AND TRAINING PLAN

APPENDIX L – PERSONNEL CONTROLS AND TECHNICAL SECURITY CONTROLS

APPENDIX M – INCIDENT RESPONSE PLAN

APPENDIX N – MEMORANDUMS OF AGREEMENT – SYSTEM INTERCONNECT AGREEMENTS

APPENDIX O – APPLICABLE SYSTEM DEVELOPMENT ARTIFACTS OR SYSTEM DOCUMENTATION

APPENDIX P – ACCREDITATION DOCUMENTATION AND ACCREDITATION STATEMENT